

AUTHENTICATION ENHANCEMENT OF RFID CARD USING AN  
ELECTRONICALLY CLIPPABLE SHIELD AND FINGERPRINT-BIOMETRICS

IKUESAN RICHARD ADEYEMI

A dissertation submitted in partial fulfillment of the  
requirements for the award of the degree of  
Master of Science (Information Security)

Faculty of Computer Science and Information Systems  
Universiti Teknologi Malaysia

JANUARY, 2012

This dissertation is dedicated to my family for their endless support and encouragement,  
and particularly, to Philip and Samson Ikuesan.

## ACKNOWLEDGEMENT

First and foremost, I would like to express my sincere gratitude to my supervisor **Dr. Norafida Binti Ithnin** for her unfading support, encouragement, and enlightenment through-out the period of this study, without whom, much effort would have been in vain and this project may have not seen fruition.

I would also want to appreciate all my colleagues in information security class, especially, those under the supervision of Dr. Norafida.

Special appreciation to all members of the Skudai Joy Gospel Chapel, a family that I will never forget.

Finally, I would like to appreciate all staffs of FSKSM, UTM and the entire UTM staff at large for the conducive learning environment.

## ABSTRACT

Radio frequency identification (RFID) is a technology that employs basic identifier of an object embedded in a chip, transmitted via radio wave, for identification. An RFID Card, responds to query irrespective of ‘*Who*’ holds the card; like a key to a door. Since an attacker can possess the card, access to such object can therefore be easily compromised. This security breach is classified as an unauthorized use of card, and it forms the bedrock for RFID card compromise especially in access control. As an authentication enhancement mechanism, this study designed and developed a method termed BIO-THENTIC Card, that integrates three existing mitigation methods which are physical clip tag, Faraday shield and fingerprint authentication; to prevent and also protect this weakness. The Bio-Thentic Card was fabricated, tested and assessed in line with the known threats, and attacks; and it was observed to proffer substantive solution to unauthorized use of RFID Card.

## ABSTRAK

Pengenalpastian frekuensi radio (RFID) adalah teknologi yang menggunakan pengecam asas objek yang tertanam dalam cip, dihantar melalui gelombang radio, untuk pengenalan. Kad RFID, respons kepada pertanyaan tanpa mengira Siapa yang memegang kad seperti kunci pintu. Sejak penyerang boleh memiliki kad tersebut, akses kepada Oleh itu, objek itu boleh dengan mudah berkompromi. Pelanggaran keselamatan ini diklasifikasikan sebagai penggunaan tanpa kebenaran kad, dan ia membentuk batu hampar untuk berkompromi kad RFID terutama dalam kawalan akses. Sebagai mekanisme peningkatan pengesanan, kajian ini direka dan dibangunkan satu kaedah yang dipanggil BIO-Kad THENTIC, yang mengintegrasikan tiga kaedah mitigasi yang sedia ada yang tag klip fizikal, Faraday perisai dan pengesanan cap jari; untuk mencegah dan juga melindungi kelemahan ini. Kad Bio-Thentic direka, diuji dan dinilai selaras dengan ancaman yang diketahui, dan serangan; dan diperhatikan untuk mengajukan penyelesaian substantiative penggunaan tanpa kebenaran Kad RFID.

## TABLE OF CONTENT

CHAPTER	TITLE	PAGE
	<b>DECLARATION</b>	iii
	<b>DEDICATION</b>	iv
	<b>ACKNOWLEDGEMENT</b>	v
	<b>ABSTRACT</b>	vi
	<b>ABSTRAK</b>	vii
	<b>LIST OF TABLE</b>	xiii
	<b>LIST OF FIGURE</b>	xiv
	<b>LIST OF EQUATION</b>	xvii
<b>1.</b>	<b>INTRODUCTION</b>	
1.1	Introduction	1
1.2	Problem Background	2
1.3	Problem Statement	3
1.4	Project Aim	4
1.5	Objective	4
1.6	Project Scope	4
1.7	Significance of the Project	5
1.8	Organization of Report	5

<b>2</b>	<b>LITERATURE REVIEW</b>	
2.1	Introduction	7
2.1.1	History of RFID technology	7
2.2	Architecture of the RFID Technology	8
2.2.1	RFID Tag	9
2.2.2	RFID Reader	10
2.3	Physical Principle Of RFID Technology	11
2.3.1	Magnetic Field Coupling: Near Field	12
2.3.2	Power Supply To A Passive RFID Tag	14
2.3.3	Antenna Impedance And Matching	15
2.3.4	Operating Frequency of RFID technology	16
2.3.5	Singulation Process	17
2.4	Communication Layers of RFID Technology	18
2.4.1	The Physical Layer	18
2.4.2	The Application Layer	19
2.4.3	The Strategic Layer	19
2.4.4	The Network-Transport Layer	20
2.5	RFID Application	20
2.5.1	Contactless Payment System	21
2.5.2	Electronic Article Surveillance (EAS) System.	22
2.5.3	Container Identification And Tracking	22
2.5.4	E-Passport And Document Identification	23
2.5.5	ChampionChip And Tag Implantation	24
2.5.6	Substitute For Bar-Code	25
2.5.7	Contactless Smart Card	26
2.5.8	Banknotes	27
2.5.9	Libraries	27
2.6	Known Challenges in RFID Technology	28
2.6.1	RFID Tag Cloning Attack	29
2.6.2	Physical Attack	29
2.6.3	Skimming Attack	30

2.6.4	Spoofing Attack	31
2.6.5	Relay Attack	31
2.3.6	Denial of Service (Dos) Attack	33
2.3.7	Clandestine Tracking	34
2.7	Counter Measures Against Known Challenges	35
2.7.1	RFID Guardian	35
2.7.2	RFID Blocker Tag	36
2.7.3	Labeling	37
2.7.4	Kill Command	37
2.7.5	RFID Zapper	38
2.7.6	RFID Clipped Tag	38
2.7.7	Faraday Cage	39
2.7.8	Authentication Protocols	39
2.7.9	Anti-Counterfeiting Technology	41
2.7.10	Physical- Layer Identification	41
2.7.11	Fingerprint Biometric Authentication	42
2.7.12	Controllable tag	43
2.8	Physical Layer Security	46
2.9	Summary of Various Mitigations and Their Drawback	44
2.10	Other Types of Mitigation Used for Physical Authentication	53
2.10.1	Iris Pattern Recognition	53
2.10.2	Body Odor Authentication	54
2.10.3	Facial Recognition	54
2.10.4	Fingerprint Pattern	55
2.10.5	Signature Pattern	55
2.10.6	Hand Geometry	55
2.10.7	Retina Pattern	56
2.10.8	Speech Pattern/Voiceprint	56
2.11	Integrating Various Physical Authentication Mitigation on RFID Card	56



2.12	Summary	58
<b>3</b>	<b>RESEARCH METHODOLOGY</b>	
3.1	Introduction	59
3.2	Operational Framework	60
3.3	Review of Existing Mitigation	61
3.3.1	Physical Clipped Tag	62
3.3.2	Faraday Cage	63
3.3.3	Fingerprint Biometric Authentication	65
3.4	Project Methodology	68
3.4.1	Phase 1: Design and Fabrication of Tag	70
3.4.2	Phase 2: Fingerprint Acquisition and Matching	70
3.4.3	Phase 3: Code Development and Testing	70
3.5	Summary	71
<b>4</b>	<b>DESIGN OF BIO-THENTIC RFID CARD</b>	
4.1	Introduction	72
4.2	Existing Mitigation Measure Analysis	73
4.3	Proposed Mitigation	74
4.4	Antenna Design	78
4.4.1	Antenna Coil	78
4.4.2	Clipped Joint	82
4.4.3	Biometric Authentication	83
4.4.4	Fingerprint Module Security Mechanism	84
4.4.5	Fingerprint Storage And Matching	85
4.5	Control Unit	86
4.5.1	AVR Atmega-8515 Microcontroller	86
4.5.2	Control Circuitry	88
4.6	Summary	91
<b>5</b>	<b>RESULT AND ANALYSIS</b>	
5.1	Introduction	92

5.2	Bio-Thentic Prototype Testing	93
5.2.1	Reader Response	96
5.2.2	Fingerprint Authentication	97
5.2.3	Tag Reading	98
5.3	Risk Assessment	98
5.3.1	Tag Manipulation	99
5.3.2	Clip Joint Circumvention	101
5.3.3	Fingerprint Manipulation	101
5.4	Risk Assessment Analysis	103
5.5	Summary	103
<b>6</b>	<b>CONCLUSION AND RECOMMENDATION</b>	
6.1	Introduction	104
6.2	Contribution	105
6.3	Future work	105
6.4	Conclusion	106
	<b>REFERENCES</b>	107
	<b>APPENDIX A</b>	
	Program code in Assembly language	117
	<b>APPENDIX B</b>	
	Program Flow Chart	138

## LIST OF TABLES

TABLE NO.	TITLE	PAGE
2.1	Summary of Attacks on RFID Layer	34
2.2	Mitigation against Attack on the Physical Layer	45
2.3	Attacks and Its Mitigation Targeted At the RFID Physical-Layer	46
2.4	Effectiveness of Mitigation to RFID Challenges	49
2.5	Comparison of Various Authentication Mitigations Based On Integrative Property with RFID Card	57
4.1	RFID Physical-Layer Attack-Mitigation Analysis	73
4.2	Instruction Command for Fingerprint Storage	85
4.3	Instruction Command for Fingerprint Match	85
4.4	Control Output Indicator	90
5.1	Test Result of Bio-Thentic Card	96
5.2	Results for Authentication Testing	97
5.3	Bio-Thentic Risk Assessment	102

## LIST OF FIGURES

FIGURE NO.	TITLE	PAGE
2.1	Typical RFID Architecture	9
2.2	Example of RFID Tag.	10
2.3	Typical of an RFID Reader	11
2.4	Lines of Magnetic Flux	12
2.5	Magnetic Loops around a Current Carrying Conductor	14
2.6	Power Supply Process for a Near Field Antenna	15
2.7	Tree Singulation Diagram	17
2.8	RFID Technology Communication Layer	18
2.9	Applicability of RFID Technology	20
2.10	A Typical Physical-Layer Security Breach in RFID System	28
2.11	New HMAC-Based Protocol	40
2.12	Authentication and Identification Framework	43
2.13	Samples of Controllable and Visible Tags.	44

3.1	Operational Framework of the Study	60
3.2	A) Schematics Of Clipped Tag B) Garment Hang Tag.	62
3.3	Clipping an Antenna	63
3.4	Operational Process of Faraday Cage.	64
3.5	Examples of Minutiae Types	65
3.6	A)Example Of An OFTIR B) Image Geometry	66
3.7	Example of a Live-Scan Fingerprint.	67
3.8	Typical Algorithm for Minutiae Extraction	67
3.9	Flow Chart of Proposed Method	69
4.1	Overview of Proposed Measure	75
4.2	Implementation Flow Chat of the Proposed Method	76
4.3	Communication process of the proposed mitigation	77
4.4	Snapshot of CST 2010 antenna design	79
4.5	FR4 lossy material	80
4.6	S-parameter of the designed antenna	81
4.7	Snapshot showing the clipped joint	82
4.8	Fabricated Antenna Unit	83
4.9	Architecture of Atmega-8515 Microcontroller	84
4.10	Block diagram of the fingerprint module	87
4.11	Pin-out of Atmega-8515 Microcontroller	88
4.12	Schematics of control process	89

5.1	Bio-Thentic Card prototype	93
5.2	Testing Procedure for Authentic User	94
5.3	Generic Testing Procedure	95
5.4	Worse case scenario of Bio-Thentic Card-physical state	100
5.5	Electrical manipulation of the clipped joint	100

**LIST OF EQUATIONS**

<b>EQUATION NO.</b>	<b>TITLE</b>	<b>PAGE</b>
2.1	Magnetic field strength	13
2.2	Energy range of RFID Tag	13
2.3	Optimal antenna coupling	13
2.4	Impedance	15
3.1	Gauss Law	64

## **CHAPTER 1**

### **INTRODUCTION**

#### **1.1 Introduction**

Radio frequency identifier (RFID) is one among series of wireless technology gaining faster and wider adoption in our today society. Unique to RFID is its portability, mobility, and flexibility in use. In a bid to make life much easier and simpler, this uniqueness has triggered its integration into our everyday life. Traditional way of identifying object/products in the retail industry; bar-code, is gradually being replace by the RFID. Of more importance to the adoption of RFID is its ability to be integrated into conveyor system, container, inventory, and transport tracking system, time sensitive application, self monitoring application such as expiry date alerts, and anti-counterfeiting of product. In addition, the relatively cheaper cost of the technology also contributes to such increasing demand.

Ironically, RFID unique properties have generated privacy concern and increasing security threats and attacks alike; which have attracted scholarly concern from researchers for the past two decades. Hence, various mitigations have been proposed to combat these challenges. Owing to the fact that the RFID system



constitutes four distinct layers (which are discussed in the following chapter), mitigations have also been structured to equate layer attacks. While the layers of the RFID system are been addressed, the physical-layer tends to receive less attention, and it has led to the success of most attacks. Researchers such as Juels (2006), Reiback (2005), Yahaya et al. (2010), e. t. c. have proposed measures to combat these attacks at the -physical-layer with focus on the reader-to-tag and tag-to-reader communication leaving the physical-layer vulnerable to unauthorized usage.

## **1.2 Problem Background**

The adoption of RFID technology into areas like physical access control have generated questions such as; ‘how can I know when my Card is being read’, how can the Card detect the authentic owner of the Card. Series of such question have trailed the stage of RFID technology.

Yahaya et al. , (2009) proposed a framework upon which a Card can identify its authentic owner using a “biometric fingerprint match on Card” and a computer system for authentication. This is also similar to the model proposed by Fons et al. , (2006).

Marquardt et al. , (2010) proposed a controllable tag system. They modeled different types of tag that can be controlled by the user at will. This is also similar to the clipped tag designed by Moskowitz et. al. ,(2007).

Zanneti et al, (2010) proposed a “physical-layer identification” system of tag based on the principle of radiometry, which was termed PARADIS. They concluded that every tag has a unique fingerprint upon which they can be distinguished.

In all of the proposed mitigation however, the question of ‘who’ (how authentic is the authentic holder of the Card) authorizes the Card is yet to be answered. Zuo, (2010) concluded that the “survivability of the RFID system” should start from the security of each tag, noting that compromising attacks emanates from the tag. Langheinrich, (2008) identified “unauthorized tag readout” as the core of RFID privacy problem stating that authenticating the interrogating parties in RFID system is a technique for privacy concern.

Therefore, the challenge of authorized Card use and reading constitutes the bane of the security and privacy issues in the RFID system. Albeit, such challenges can be protected against by proposing an enhance authentication system particularly, at the user-end on the physical-layer of the RFID system.

### **1.3 Problem Statement**

Attacks on the physical-layer of the RFID system have received minimum combative measure leading to the discouraging rate of attacks on it. Some of the existing measure tend to offer mitigation but failed to consider the authenticity of the user at the tag end of the system. Considering these limitations, satisfactory answers to the questions listed below needs to be purveyed in the process of this study:

- i. How authentic is the authentic Cardholder?
- ii. How can an authentic Cardholder dictate Card responds to interrogation?
- iii. How can an authentic Cardholder know when the tag is being read?
- iv. What happens to the confidentiality of the Card when it is stolen?
- v. How will this proposed method be evaluated, with respect to authentic authorization?

## **1.4 Project Aim**

The aim of this study is to improve the security level of the RFID system at the physical layer as well as ensure confidentiality in the use of RFID Cards by enhancing authentication of user at the tag end.

## **1.5 Project Objectives**

In order to accomplish the aim of this study; the following objectives must be achieved:

- i. To study and investigate existing mitigation measures on security and privacy of the RFID system with reference to the physical-layer.
- ii. To propose an enhanced authentication mechanism for authenticating user at the tag-end of the RFID system
- iii. To implement the proposed authentication mechanism and evaluate its effectiveness

## **1.6 Project Scope**

The following defines the scope of this study:

- 1) This study entails security issues relating to the physical-layer of a passive and semi-passive tag used in contactless Cards.

- 2) The proposed enhancement method will be based on three existing mitigation methods, which are clipped tag, Faraday cage and fingerprint biometric authentication.
- 3) The designs and fabrication of the system is limited to the physics of the tag antenna and not on the detail of the RFID tag itself.

## **1.7 Significance of the dissertation**

In this study, various mitigation measures for combating the challenges of the RFID system will be discussed. Furthermore, detailed analysis will be carried out on the specific three chosen measures, which will give insight to other researchers. The challenges of unauthorized tag read, tag use and even tag killing will receive appropriate mitigation.

## **1.8 Organization of report**

This thesis comprises chapters arranged in the numeric order of 1 to 6. The detail of each chapter is detailed as follows;

**Chapter 1** of this report gives the overview of this study, problem background, objective, scope, and problem statement of this study.

**Chapter 2** of this report covers the history and basic theory of the RFID technology as well as its importance in various areas of application. Security and privacy challenges and existing mitigation in the RFID system were also discussed in detail.

**Chapter 3** describes the research methodology of this study. In addition, it also discussed the project methodology for the study.

**Chapter 4** of this report covers the design and fabrication process upon which the proposed methodology was framed.

**Chapter 5** of this report discussed the result of the design and fabrication process. It also discussed result of risk assessment carried out on the fabricated prototype.

**Chapter 6** covered the conclusion and recommendation proffered in this study.